SECTION 1
ADDENDUM B
CONDUCTING ALTERNATIVE INTERNAL CONTROL REVIEWS

Alternative Internal Control Reviews, used for programs determined to be low risk and some medium risk, are usually narrow in scope and focus attention on controls over areas or activities of a component which have the highest potential for ineffective or inefficient operation or loss of government resources. Such reviews may be combined with other review processes (such as internal control or technical reviews) or be conducted as a separate review. Where periodic reviews of programs, organizations, or functions are conducted by bureaus, PFM strongly encourages combining internal control reviews (financial and programmatic), GPRA/PART performance assessments, and other internal bureau reviews to avoid duplication of effort and to make them more acceptable to managers. **Bureaus are also encouraged to use the DOI automated assessment approach to review a component's controls. The automated assessment incorporates eight management integrity measures based on OMB's and GAO's objectives and standards for internal controls in federal programs and administrative functions (see page IC-33 in this appendix).** Additionally, combining reviews will help institutionalize the internal control processes within the Department.

The Department has decided that Internal Control Reviews (ICR) are to be done on all controls or program areas considered to be of high risk. Since an ICR requires a description of all event cycles and analysis of control objectives and techniques, testing is normally very detailed and extensive. When the level of risk for controls or program areas is considered to be low, the Department has decided that an Alternative Internal Control Risk is appropriate because it is generally less paper intensive and more cost effective and efficient. For program areas considered to be medium risk, it is management's discretion as to whether the ICR or AICR is more appropriate; the decision to use the ICR or AICR should be based on the visibility of the program, the dollar impact of the program on outside entities (public or governmental), etc.

Suggested steps for conducting AICRs are listed below.

START THE EVALUATION

Plan the Evaluation

The AICR should be carefully planned to gain managerial support and to ensure that the objectives are accomplished. The planning process should include the following tasks:

Determine scope and objectives. Consider whether the purpose of the AICR is to perform a comprehensive review of controls over all the high risk areas or if it is to perform a limited review of one aspect of the component.

Assign staff. The team members selected should be knowledgeable of the program area, have analytical skills, and be trained in conducting control evaluations. Ideally, team

members should be selected from within the responsible program office and from an independent "program-evaluation" function. The number of reviewers should be based on the complexity and scope of the review.

Allocate staff resources and establish timeframes. It is helpful to allocate the minimum and maximum amount of staff resources to be used for completing each task. The final planned completion date should be set with interim planned completion dates for each review task.

Analyze the General Control Environment

The purpose of analyzing the general control environment is to determine if management's attitude is conducive to a strong internal control system. The analysis of the general control environment will provide the reviewer with a preliminary opinion about the effectiveness of specific controls. If an analysis has been previously completed, check to see if it is still accurate and update, as necessary.

The factors that influence the general control environment are:

- Organization;
- Delegation of authority;
- Policies and procedures;
- Personnel;
- Planning, Budgeting and Accounting; and
- Reporting.

Exhibit 1 is a worksheet to use in analyzing the general control environment.

Analyze Information Technology

If the component contains an IT application, it should be analyzed to determine if IT application controls should be reviewed. This review of IT can be a separate review or part of the AICR. An IT application should be included if it contains any of the following characteristics:

- Processes information used for significant management decisions;
- Calculates or records amounts owed by or to the Government;
- Maintains balances or other records used to control government resources;
- Maintains or processes information necessary for effective and efficient program operation; or
- Maintains or processes sensitive information.

NOTE: Section 3, Chapter 3, Executing ICR for Information Systems and IT Programs, of this handbook provides additional details on this process.

DEFINE CONTROL SYSTEMS

Identify and Document High Risk Areas

The reviewer should identify those risks which are high for the component as a whole. High risks are potential unwarranted occurrences which, if they occur, would prevent a component from reaching its objectives or would result in a significant loss of government resources. When identifying high risk areas, the reviewer should also consider the probability of the unwanted occurrence and the severity of the consequences. Exhibit 1 is a worksheet for identifying and documenting high risks

Identify and Document Control Techniques

Control techniques are a series of carefully constructed checks and balances designed to provide reasonable assurance that the control objectives are met in an efficient and effective manner. Control techniques should be observable and cost effective. Examples of control techniques include passwords to limit access to databases, written delegations of authority, technical reports, documentation of processes and procedures for carrying out program and technical activities, periodic supervisory reviews, comparisons of actual results to planned results, and segregating sensitive duties among several individuals.

When developing control techniques, it is crucial to identify the relationship between the techniques and the risks within the event cycle. Control techniques are implemented to reduce risks and meet the control objectives.

Control techniques are the basis of testing. Testing verifies compliance with existing control techniques to determine if the controls are operating as intended and are sufficient to provide reasonable assurance of achieving the control objectives.

Compare Control Systems to the GAO Control Standards

The GAO control standards **(web site address www.gao.gov)** define the minimum level of quality acceptable for an internal control system. These standards apply to all operations and functions except development of legislation, rulemaking, or discretionary policymaking. The five GAO standards for internal control are: (1) Control environment; (2) risk assessment; (3) control activities; (4) information and communications; and (5) monitoring. These standards define the minimum level of quality acceptable for internal control in government programs and administrative operations and provide the basis against which internal control is to be evaluated. The standards apply to all aspects of an agency's operations—programmatic, financial, and compliance.

NOTE: The term internal control as used in the GAO standards is synonymous with the term management control as it was used in the prior version of OMB Circular A-123.

The GAO standards provide a general framework for internal controls. Agency/bureau management is responsible for developing the detailed policies, procedures, and practices to fit their operations, and ensuring that internal controls are built into and are an integral part of operations. A more detailed description of the standards follows.

- Control Environment**.** Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management.

- Risk Assessment**.** Internal control should provide for an assessment of the risks the agency faces from both external and internal sources. Risk assessment is the identification and analysis of relevant risks associated with achieving the objectives, such as those defined in strategic and annual performance plans developed under the GPRA, and forming a basis for determining how risks should be managed.

- Control Activities**.** Internal control activities help ensure that management's directives are carried out. The control activities should be effective and efficient in accomplishing the Department's control objectives. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives, such as the process of adhering to requirements for budget development and execution. They also help ensure actions are taken to address risks. Control activities include approvals, authorizations, verifications, reconciliations, performance reviews, maintenance of security, and the creation and maintenance of related records which provide evidence of execution of these activities along with supporting documentation. Examples of control activities include:

    - Top level reviews of actual performance;
    - Reviews by management at the functional or activity level;
    - Management of human capital;
    - Controls over information processing;
    - Physical control over vulnerable assets;
    - Establishment and review of performance measures and indicators;
    - Segregation of duties;
    - Proper execution of transactions and events;
    - Accurate and timely recording of transactions and events;
    - Access restrictions to and accountability for resources and records; and
    - Appropriate documentation of transactions and internal control.

- Information and Communications**.** Information should be recorded and communicated to management and others within the entity who need it and in a form and within a timeframe that enables them to carry out their internal control and other responsibilities.

- Monitoring**.** Internal control monitoring should assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved.

TEST THE CONTROL SYSTEM

Testing verifies the effectiveness of control techniques in operation by determining if they are, in fact, operating as intended, meeting the control objectives, and reducing risks. By testing, the responsible official can quickly validate whether: (1) Prescribed procedures are performed in accordance with instructions; (2) procedures are performed by personnel having no incompatible duties; (3) actual transactions processed in the operation are in fact those authorized for the group; and (4) actual operations are conducted in accordance with the control objectives and techniques which have been devised for the component.

The focus of testing should be upon the highest potential for ineffective or inefficient operation or loss of government resources and those areas of inadequate internal control system design. Testing consists of the following steps.

Select Controls to be Tested

It is both impractical and unnecessary to test all control techniques. The control techniques to be tested should be those that contribute most to achieving the control objectives or managing the risk. A control should be eliminated from testing when: (1) The technique does not meet the control objective or manage the risk because it is poorly designed, unnecessary, duplicative, or is not performed in a timely manner; and (2) The cost of testing exceeds the value of the technique being tested. If a technique is excluded from testing, the reasons supporting this decision should be recorded.

Select Test Methods

Testing methods include:

- Document analysis - reviewing existing records, completed forms, or other documentation;
- Transaction testing - entering and processing transaction data through the system or tracing transactions through the system;
- Observation - watching the performance of specific control techniques; and/or
- Interview - eliciting information from the personnel who perform the control technique.

Tests should not be limited to information obtained through interviews, but interviews should be used to supplement document analyses and/or observation. One or more methods of testing may be combined during the test.

As mentioned in Chapter 2, the Automated Assessment Approach is considered an AICR which can assist bureaus in reducing their costs for conducting reviews and reporting the results. The primary benefits of the automated assessment are that it provides: (a) A targeted and focused

approach for control evaluations; (b) a concise and meaningful summary report for management; (c) an effective means of identifying and reporting best practices; (4) a view of assessment results (strengths and weaknesses) for all measurement areas at one glance; and (5) an effective means of tracking and reporting trend information over time. The assessment is performed electronically using an off-the-shelf surveying and analytical software tool (Survey Tracker) that provides diagnostic and executive-level reporting. Bureaus have the discretion to determine how many of the eight management integrity measures will be tested.

The survey assessment questionnaire is built around the eight integrity measures that support the general and specific internal control standards delineated in OMB Circular A-123 and incorporated in GAO's "Standards for Internal Control in the Federal Government." The eight management integrity measures follow.

- Organizational Control Environment. The objective of this measure is to ensure that an organization's goals, objectives, policies, and procedures are conducive to achieving sound internal controls, and that the organization places a high level of importance on management's integrity and ethics. The organizational control environment sets the tone for and influences the internal control consciousness of its employees. It also provides the foundation for the internal control structure. Organizational control environment factors include: employees integrity, ethical values, and competence; management's philosophy and operating style; management's methodology to assign authority and responsibility, and to organize and develop staff; management's planning, budgeting, accounting and reporting; and senior management direction.

- Risk Management**.** The objective of the risk management measure is to ensure that an organization identifies, assesses, and considers the consequences of events that could prevent the achievement of its goals and objectives, and/or result in significant loss of resources. Every organization faces a variety of risks from external and internal sources and changes in its operating environment. These risks should be continuously monitored and assessed.

- Program Effectiveness**.** The objective of this measure is to ensure that management plans and allocates sufficient resources to programs to achieve intended results. Further, the program effectiveness measure embraces the idea that organizations have strategic planning systems that employ performance measurement systems to provide for comparisons of planned outcomes and results against actual outcomes and results.

- Resource Stewardship. The objective of this measure is to ensure resources are safeguarded and managed in a manner consistent with the mission of the organization. Access to resources should be limited to authorized individuals, and accountability for the custody and use of resources should be assigned and maintained.

- Regulatory Compliance. The objective of this measure is to ensure that laws and regulations are followed. Management and staff must be aware of and ensure that all

programs, operations, obligations, and costs incurred comply with applicable laws, regulations, and executive orders.

- Audit Resolution**.** The objective of the audit resolution measure is to ensure that organizations take prompt and responsive action on all audit findings and recommendations in order to improve program and organizational efficiency and effectiveness. Responsive action is that which corrects identified deficiencies. Where audit findings identify opportunities for improvement rather than cite deficiencies, responsive action is that which produces improvements.

- Management Information**.** The objective of this measure is to ensure that reliable and timely information is obtained, maintained, reported, and used for decision-making at all levels. Information systems should produce reports containing program, operational, financial, and compliance related data, to effectively manage and control the programs and operations of an organization.

- Financial Systems and Data Integrity**.** The objective of the financial systems and data integrity measure is to ensure that an organization's financial management system and related operations conform with Government-wide principles, standards, and requirements, and that the process of managing information necessary to support program and financial managers, and assuring data captured and reported is complete, accurate, accessible, timely, and usable.

NOTE: A sample survey assessment questionnaire is included as an Exhibit.

Determine Amount of Testing

It is unrealistic to observe every control used or review 100% of the records at each location. The reviewer must select the organizations and locations where the tests will be conducted and select a sample (using appropriate sampling techniques) for each control to be tested.

Plan Data Collection

Accurate recording of test results is an extremely important part of the testing process. A data collection plan assists in determining how to record the test results. For example, interview guides should be used to ensure that all areas of concern are covered.

Conduct the Tests

While conducting the tests, follow the sample plan unless a decision is made to review the scope or size of the sample based on the results of the initial sample. Increase the sample size if the initial tests provide mixed results. When possible, retain copies of authorizing documents or other physical evidence that control techniques are working.

A control is not effective when the assessment determines it is not adequately designed or when it is reviewed and determined that it is not functioning effectively. There is a control gap when a control does not exist for a given assertion, when a control does not adequately address a relevant assertion, or a control is not operating effectively. Reviewers should always determine that other compensating controls do not exist that would mitigate the risk.

NOTE: Watch for compensating controls. Sometimes a control technique will appear to be weak or not operating. In such a case, determine if personnel are compensating for the shortcomings by using informal control mechanisms. Control mechanisms being used need to be evaluated and documented during the testing.

Analyze Test Results and Develop Conclusions

The tests of specific control techniques must be analyzed to determine if the degree of compliance with control techniques is adequate. It is important to remember that several control techniques are usually utilized to meet a control objective or manage a risk. Accordingly, the failure to substantially comply with one individual control technique does not necessarily result in a failure to meet the control objective or manage a risk.

The test results should then be discussed with managers responsible for operating the control techniques at the location or organization that was reviewed. These discussions will: (1) Communicate the results of the tests and any conclusions drawn; (2) Seek agreement on those conclusions; and (3) Elicit recommendations from managers on any necessary corrective actions. Such discussions are best held as soon as the testing and related analyses of results are completed.

If you used the Automated Assessment Approach, the results of the survey questionnaire (questions based around the eight management integrity measures and other program or administrative policies and procedures) and responses are analyzed by the Survey Tracker software and a graphical summary report, known as a spider diagram, is produced. The summary report presents the actual assessment against a Department or bureau defined standard for each management integrity measure (as shown in the spider diagram contained in the Case Studies). The closer the results of the actual assessment for each measure are to the defined minimum standard of each integrity measure or to the center of the spider diagram, sufficient internal controls for the program (or activity evaluated) are in place and working. The further from the center the minimum standard set for each integrity measure, the weaker the internal controls. Managers should use results to strengthen internal controls where needed in their areas of responsibility or do additional targeted testing.

Each internal integrity measure area is of equal importance and managers should use the spider diagram to determine the strong and weak internal control areas. Managers should work toward achieving balance between the areas to foster continuous improvement through benchmarking, training, and outreach programs with emphasis on accountability.

Develop Plans for Corrective Action

The primary purpose of the control evaluation process is to assist managers in identifying and correcting weaknesses. When a weakness is found, a decision must be made to institute new controls, improve existing controls, or accept the risk inherent with not correcting the weakness (unless the weakness surpasses established materiality thresholds). The decision must be documented in the evaluation's corrective action plan.

The following information should be completed while preparing corrective action plans (Refer to Chapter 4, Developing and Implementing Corrective Actions, for detailed requirements).

- Summary Description of the Weakness/Deficiency
- Year First Identified
- Target Correction Date
- Accountable Official
- Funding/Resources Required to Resolve the Weakness/Deficiency
- Summary of Corrective Actions
- Quarterly Corrective Actions
- Metrics

REPORT THE RESULTS

Control evaluation results for each component should be summarized in a report. The report should identify control weaknesses and describe plans for corrective action. Since the report forms the basis for the certification required by FMFIA, it must provide the bureau head and assistant secretary with sufficient assurance that the review was conscientiously performed and accurately reflects the condition of internal controls.

The report should contain all control weaknesses which are significant to the next higher organizational level, regardless of the process through which the weaknesses were identified. All sources of information on the status of controls, such as audit reports, management reviews, and routine management reports, are to be considered in identifying control weaknesses. The transmittal memorandum should describe: (1) The risks that the evaluation focused on; and (2) the testing conducted, locations, controls techniques tested, and type and amount of testing.

The report should be submitted to the official designated as the responsible official for component controls and their evaluation. After review by the responsible official, the report is to be transmitted to the bureau ICC for approval by the bureau head. The report must be approved by the bureau head and appropriate program assistant secretary and submitted to PFM with a copy to the OIG.

DOCUMENT THE EVALUATION

Documentation is written material explaining the operation of the control system and the conduct of an internal control assessment. GAO specific control standards require that all internal

controls and all transactions and other significant events are to be clearly documented and the documentation is to be readily available for examination. In addition, responsible officials should prepare and maintain sufficient documentation to evidence the conduct of an internal control assessment and the basis for the results and conclusions reached. This documentation should include written evidence concerning:

- The officials participating in the review;
- The risks reviewed;
- The control examined;
- The extent and type of control tests performed;
- The analysis of the tests conducted;
- A description of any weaknesses found;
- The actions recommended to correct the weaknesses; and
- The responsible official.

System documentation provides a means of communicating information on the operation of the control system and serves as a standard to measure the operation of the control system. It further provides information necessary for supervisory or other review and serves as a basis for training new personnel. Assessment documentation provides evidence that an internal control assessment was performed and provides support for the reasonable assurance determination. It serves as the basis for supervisory review and quality control while assisting in subsequent assessments.

How much documentation is enough? Sufficient system documentation answers why the system was designed, what the system does, and how the system operates. Sufficient evaluation documentation answers who did what, what were the results, and why were actions taken?

NOTE: Sufficient documentation should not involve an inordinate amount of paper. However, when testing financial reporting internal controls sufficient documentation must be available to demonstrate the bureaus assessment.